Exploring Energy Efficiency of Lightweight Block Ciphers - DTU Orbit (09/11/2017)

Exploring Energy Efficiency of Lightweight Block Ciphers

In the last few years, the field of lightweight cryptography has seen an influx in the number of block ciphers and hash functions being proposed. One of the metrics that define a good lightweight design is the energy consumed per unit operation of the algorithm. For block ciphers, this operation is the encryption of one plaintext. By studying the energy consumption model of a CMOS gate, we arrive at the conclusion that the energy consumed per cycle during the encryption operation of an r-round unrolled architecture of any block cipher is a quadratic function in r. We then apply our model to 9 well known lightweight block ciphers, and thereby try to predict the optimal value of r at which an r-round unrolled architecture for a cipher is likely to be most energy efficient. We also try to relate our results to some physical design parameters like the signal delay across a round and algorithmic parameters like the number of rounds taken to achieve full diffusion of a difference in the plaintext/key.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , University of Lugano
Authors: Banik, S. (Intern), Bogdanov, A. (Intern), Regazzoni, F. (Ekstern)
Pages: 178-194
Publication date: 2016

Host publication information

Title of host publication: 22nd International Conference on Selected Areas in Cryptography (SAC 2015) : Revised Selected Papers
Publisher: Springer
Editors: Dunkelman, O., Keliher, L.
ISBN (Print): 978-3-319-31300-9
ISBN (Electronic): 978-3-319-31301-6

Series: Lecture Notes in Computer Science
Volume: 9566
ISSN: 0302-9743
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences
Conference: 22nd International Conference on Selected Areas in Cryptography, Sackville, Canada, 12/08/2015 - 12/08/2015
AES, Lightweight block cipher, Low power/energy circuits
DOIs:
10.1007/978-3-319-31301-6_10
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016